PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-249889
(43)Date of publication of application : 17.09.1999

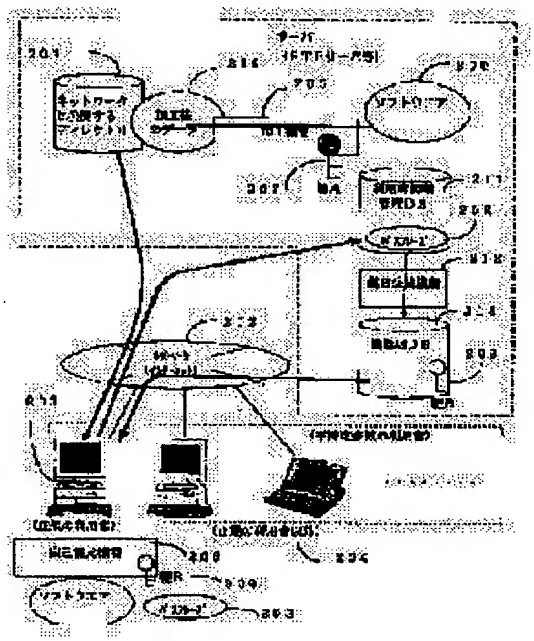
(51)Int.Cl. G06F 9/06

(21)Application number : 10-050316
(22)Date of filing : 03.03.1998

(71)Applicant : HITACHI LTD
(72)Inventor : TOMIZAWA SATOSHI

(54) PROGRAM FOR DISTRIBUTING SOFTWARE BY USING NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the software usage by an illegal user and to prevent the convenience of a user from burring by providing a function for generating second keys existing at every user from the previously registered pass phrase of the user and the key and a key managing database for registering the second keys.
SOLUTION: The user registers his pass phrase 208 in the user information managing database 211 of a server together with his information (an address and a name, etc.), 11. When the pass phrase 208 is registered, the key B generating function 212 at the side of the server fetches the keys A and the pass phrases 208 at every user, generates the keys B 209 at every user and registers them in the key managing database 213. When the register of the keys B209 at every user is ended, a mail is transmitted from a server operating organization or automatically transmitted by the register function to the user. Thus, danger that the keys B 209 are tapped simultaneously with the pass phrases 208 is avoided and the user can always use a software by using a network.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－249889

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｃ
			５５０Ｚ

審査請求　未請求　請求項の数５　ＯＬ　（全６頁）

(21)出願番号　特願平10－50316

(22)出願日　平成10年(1998)３月３日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

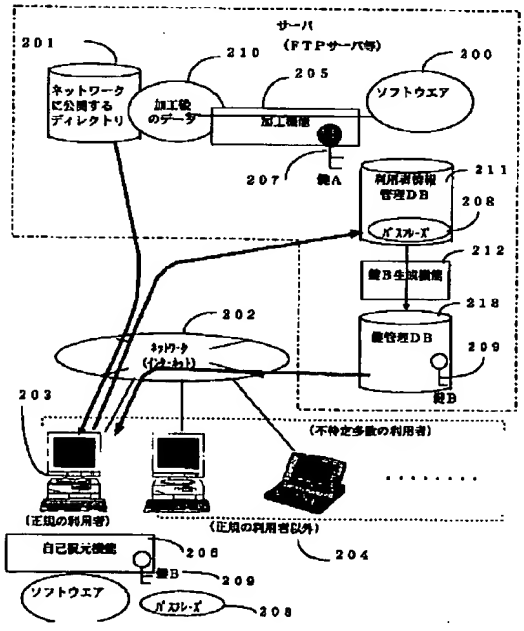
(72)発明者　富澤　智
神奈川県川崎市幸区鹿島田890番地株式会社日立製作所情報システム事業部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　ネットワークを利用してソフトウェアの配布を行う為のプログラム

(57)【要約】
【課題】ネットワーク上のソフトウェアの保護はインストール時のパスワードを郵送などの人的手段で行っており処理の自動化など運用方法が確立されていない。またインストール時のパスワードはソフトウェアに括り付けであり正規の利用者により漏洩した場合不正使用の統制ができない。
【解決手段】本発明ではネットワークを利用したソフトウェアの加工、復元方法およびその中でのセキュリティ確保を利用者毎のパスフレーズと鍵を使用することによりソフトウェアの不正使用を防ぎ、また鍵などが漏洩した場合サーバ側で不正使用をある程度統制することを可能とした。また利用者の利便性を損なわずサーバの管理者が利用者単位かつソフトウェア単位に利用可否を管理できる簡易な方法を提供した。

図２



1

【特許請求の範囲】

【請求項１】インターネット等の不正利用者を容易に把握できないネットワークに接続された複数のクライアントコンピュータおよびサーバコンピュータを含む構成で、クライアントコンピュータに組込まれるソフトウェアの配布においてサーバ側で動作する特定の鍵を使用したソフトウェアの加工機能とクライアント側で動作する特定の鍵を必要とするソフトウェアの復元機能とサーバ側において予め登録された利用者のパスフレーズと鍵から利用者毎に存在する第二の鍵を生成する機能と生成した第二の鍵を登録する鍵管理データベースとを提供することにより正規のソフトウェア利用者以外の不正使用防止を実現するプログラム。

【請求項２】請求項１記載のサーバ側の利用者管理データベースとクライアント側のソフトウェア復元機能の連携によってソフトウェアの復元状態をサーバ側で利用者毎に管理し、正規の利用者のソフトウェアの組込みを複数のクライアントコンピュータに行わせないよう管理するプログラム。

【請求項３】請求項１記載のサーバ側の利用者管理データベースとクライアント側のソフトウェア復元機能の連携によってソフトウェアの復元状態をサーバ側で利用者毎に管理し、正規の利用者のライセンス数以上のソフトウェア利用を行わないよう管理するプログラム。

【請求項４】請求項２、３記載のソフトウェアの復元状況を把握する機能によりソフトウェア不正使用の状況を把握するプログラム。

【請求項５】請求項１記載の利用者のパスフレーズの登録をソフトウェアをダウンロードするネットワークとは別のメディアを利用して行うことにより安全性を高める方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はネットワークに接続された複数のクライアントコンピュータおよびサーバコンピュータを含む構成で、サーバコンピュータからクライアントコンピュータに組込まれるソフトウェアの配布を安全に行う方法に関し、特にインターネットなどのような不特定多数の利用者が存在するネットワークを利用したプログラムの配布を安全に行う方法およびプログラムに関する。

【０００２】

【従来の技術】パソコン等のソフトウェアの販売・配布において可搬媒体によるもの、およびネットワークを利用したものが一般的である。これらの配布においてはコピープロテクト（媒体を簡単にコピーできないようにする技術）およびインストールプロテクト（ソフトウェア組み込み時に特定の記号、番号の入力を必要とし複数の人が機器に組み込むことを防止する技術）あるいは起動時に特定のパスワードを必要とする方法（特願平4-1373

2

09）により正規の購入者にのみ利用させるよう保護される。これに対して不特定多数が接続するネットワーク上（インターネットが代表的である）のソフトウェアの配布においては、ソフトウェアの一部または全部がネットワーク上のサーバに公開され自由に利用者が取得できる。ソフトウェアの一部の配布では予め正規の利用者が購入済のソフトウェア本体がなければ利用できないという思想のもと自由な取得を許している。ソフトウェアの全部の配布では試用版のソフトウェアなどに代表される無償のソフトウェアあるいはそれに準じる安価なソフトウェアに限られる。安価なソフトウェアの場合は代金の回収を保証しないなどの方法で回避している。

【０００３】

【発明が解決しようとする課題】かかる従来の方法においては次のような課題がある。

【０００４】すなわち①従来の認証技術を利用したサーバ／クライアントの安全な接続ではサーバとクライアントの接続を第三者から保護することを目的としておりサーバ内に置かれたクライアントに公開するディレクトリ上のソフトウェア全てを一律公開するかしないかのどちらかの管理しかできない。つまりソフトウェアの利用可否をソフトウェア単位かつ利用者単位に管理し、購入した正規の利用者にのみ公開するということができない。

【０００５】②ネットワークで取得したソフトウェアのインストールプロテクトのパスワードを別のメディア（例えば郵便物など）により正規の利用者に知らせるなどの方法によりソフトウェアの利用を保護している場合があるがサーバ側の運営者の人手により行われるため誤りも起きやすい。またこの方法ではソフトウェアに1つのインストールプロテクトのパスワードしか設定できず利用者の過失によりインストールプロテクトのパスワードが漏洩すると不正利用が統制できない危険性がある。

【０００６】

【課題を解決するための手段】本発明は、ネットワーク上で公開するソフトウェアを組込むためのプログラムおよびソフトウェアを構成する部品（以下インストーラと記述）を公開するときに特定の鍵（鍵Ａ）を使用して加工し、ソフトウェアを購入した正規の利用者に対してその加工したものを復元するために使用する鍵（鍵Ｂ）を渡すことにより、正規の利用者による復元を可能とし、鍵Ｂを持たない不正使用者によるソフトウェアの使用を事実上不可能とする。配布対象のソフトウェアはソフトウェア毎に存在するある一つの特定の鍵（鍵Ａ）により加工する。サーバ側では利用者情報を管理するデータベースとして、利用者を特定するＩＤと利用者が購入したソフトウェアの情報と鍵Ｂを格納するデータベース（利用者情報管理データベース）および利用者を特定するＩＤと利用者の個別情報（パスフレーズ）を格納するデータベース（パスフレーズ登録データベース）を保有する。これらのデータベースはそれぞれ利用者によるアク

セスを個別に制御し、前者は利用者による検索のみを許可し、後者は利用者による利用者の個別情報（パスフレーズ）の登録のみを許可する。パスフレーズはパスワードよりも比較的長くパスワードのように利用者以外に知られない情報である。サーバ運営者は正規の利用者の登録、利用者毎の鍵Ｂの生成を行いデータベースに登録する。利用者は利用者の個別情報をサーバに登録する。サーバ側では利用者の個別情報により鍵Ａを加工し鍵Ｂを生成する。このとき鍵Ｂに利用者の個別情報を与えることにより生成したときと逆の計算によって鍵Ａを求めることができるものとする。鍵Ｂはサーバを運営する組織から利用者に対して渡される。渡す方法としては①利用者がサーバにオンラインで接続してサーバのＤＢに利用者ＩＤを与えることにより検索し取得する方法。セキュリティ確保のため、このとき与える利用者のＩＤは基本的には上記個別情報とは異なるものとする。②サーバ運営者から郵送で鍵Ｂを利用者に送る方法。などが考えられる。利用者は取得した鍵Ｂとサーバに登録した利用者の個別情報をソフトウェアのインストーラに与えることにより鍵Ａを再生成しソフトウェア復元する。安全のためソフトウェアの復元が正常に完了した場合はクライアントＰＣ上から鍵Ｂを自動的に消去する。サーバ運営者は鍵Ａが漏洩した場合またはある特定の頻度で鍵Ａを変更することによりソフトウェアの不正利用を防止する。また利用者により鍵Ｂと利用者の個別情報が漏洩したことがわかった場合はデータベース上から鍵Ｂと利用者の情報を削除する。

【０００７】また、本発明においては利用者のパスフレーズの登録をソフトウェアをダウンロードするネットワークとは別のメディアを使って行うことにより、安全性の向上が可能である。この場合の別のメディアとは販売店店頭での専用回線を使った登録、暗号化技術を使った信頼性の高いネットワーク等が適用できる。この方法は従来のインストールプロテクトのパスワードを別のメディアを使って利用者に知らせる方法とは異なる。従来の方法では一律共通のパスワードを設定するため利用者による漏洩での影響が大きいが、本発明の方法を用いれば不正利用に対しての把握及び対策が可能である。また本発明の方法ではソフトウェアダウンロードに使用するネットワークと別のネットワークを販売店の店頭等に設置することによりソフトウェアサポートの利用者登録と同時に行うことができ利用者の利便性を損なうことがない。

【０００８】

【発明の実施の形態】以下本発明実施の具体的方法を示す。

【０００９】図１は本発明を適用する前の環境を示す。不特定多数が接続するネットワークの典型的な例としてインターネットを示している。この環境においてソフトウェア１００はサーバ上のネットワークに公開するディレクトリ１０１に格納されネットワーク１０２を通じて正規の利用者１０３またはそれ以外の利用者１０４にダウンロードされ利用される。この場合正規の利用者とそれ以外を区別できない。

【００１０】図２は本発明の概要を示す。本発明において追加される機能はサーバ側の加工機能２０５およびクライアント側の復元機能２０６である。まずソフトウェア２００は鍵Ａ２０７をパラメータとし加工機能２０５により加工されソフトウェア加工後のデータ２１０となる。加工機能２０５はデータ伝送時間を考慮して圧縮機能を含んでいる方が望ましい。加工後のデータ２１０はネットワークに公開されるディレクトリ２０１に格納される。利用者がソフトウェアを購入し正規の利用者として登録を申請すると正規の利用者として利用者情報管理データベース２１１にサーバ運営者により登録される。利用者は自分の情報（住所、氏名等）とともに利用者のパスフレーズ２０８をサーバの利用者情報管理データベース２１１に登録するよう申請する。登録の申請の方法は①店頭による申請②オンライン申請などが考えられる。利用者情報管理データベース２１１へのパスフレーズ２０８の登録は正規の利用者として利用者情報管理データベース２１１に登録されている利用者に限られる。パスフレーズ２０８が登録されるとサーバ側の鍵Ｂ生成機能２１２は鍵Ａと利用者毎のパスフレーズ２０８を取り込み利用者毎の鍵Ｂ２０９を生成し鍵管理データベース２１３に登録する。利用者毎の鍵Ｂ２０９の登録が完了したらサーバ運営組織からのメールまたは登録機能が自動的に利用者にメールを送信する。あるいは利用者の登録後一定の期間経過したらソフトウェアが利用できることを予め利用者に知らせておく。

【００１１】ソフトウェアが利用可能であることを知った利用者はネットワークでサーバに接続しネットワークに公開するディレクトリ２０１からソフトウェアの加工後のデータ２１０をダウンロードする。加工後のデータ２１０は自己復元機能２０６を内蔵しており自己復元機能２０６を起動すると利用者のパスフレーズ２０８を取り込むとともにサーバに接続し鍵管理データベース２１３から利用者毎の鍵Ｂ２０８を取得し、これらから鍵Ａ２０７をクライアントコンピュータ内で再生成する。このときパスフレーズはクライアントコンピュータ内から外に出ない。つまり鍵Ｂ２０９とパスフレーズ２０８が同時に盗聴される危険を回避する。次に鍵Ａ２０７を使用しソフトウェアを復元する。ソフトウェアの復元が完了したら鍵Ａと鍵Ｂをクライアントコンピュータ内から消去する。利用者の立場から見ればソフトウェアを購入し正規の利用者登録が完了した後はネットワークを利用していつでもソフトウェアを利用できることになる。また鍵Ｂの取り込みはネットワークに接続されていれば良く、利用者は意識する必要がない。サーバ運営者から見ればソフトウェアの正規の利用者を登録すれば後は自動

化が可能である。正規の利用者以外のソフトウェアの使用は利用者のパスフレーズ２０８および鍵Ｂ２０９が同時に漏洩しない限り保護される。パスフレーズ２０８および鍵Ｂ２０９はネットワーク上で容易に盗聴できないよう暗号化技術などの併用により保護することが望ましい。特にパスフレーズ２０８の登録は別のネットワーク（販売店とサーバ間のみ接続可能なネットワーク）または郵便物などを利用することもできる。

【００１２】また次のようにすれば正規の利用者による複数のコンピュータへのインストールを防ぐことができる。クライアントでソフトウェアの復元が完了した場合サーバに通知し、サーバの利用者情報管理データベースにソフトウェアが使用中の状態であるということを登録する。利用者が別のコンピュータにソフトウェアを組込みたい場合は既に組込まれているコンピュータでアンインストールを行いアンインストールの機能がサーバにアンインストールが完了したことを通知しサーバの利用者管理データベースがソフトウェア未使用中になるようにすれば良い。

【００１３】以下それぞれの機能について図３、図４を用いて詳細に説明する。

【００１４】加工処理では、まず入力となる鍵Ａおよびソフトウェアを用意し加工処理開始３００を起動する。次にカウンタークリア３０１した後、鍵Ａの取り込み３０２をし入力ファイルを１ブロックずつ読み取り鍵Ａを使って加工する。（３０３から３０９）３０５でＥＯＦ（入力データの終了）を判定しＥＯＦとなったら、最後に自己復元機能を出力データに付加３１０し処理を終了する。復元処理では、まず入力となる鍵Ｂを用意し復元処理開始４００を起動する。次にカウンタークリア４０１した後、パスフレーズの取り込み４０２し、ネットワークと接続４０３し、鍵Ｂをサーバ上の利用者情報管理データベースから取得する。取り込んだ鍵Ｂとパスフレーズから鍵Ａを再生成４０５し、入力ファイルを１ブロックずつ読み取り鍵Ａを使って復元する（４０６から４１２）。４０８でＥＯＦ（入力データの終了）を判定しＥＯＦとなったら処理を終了する。

【００１５】

【発明の効果】以上述べたように、本発明によればネットワークにおけるソフトウェアの配布において正規の契約をしていない不正使用者がソフトウェアを利用できないように保護することができ、また利用者の利便性を損なわずサーバの管理者が利用者単位かつソフトウェア単位に利用可否を管理できる簡易な方法を提供できる。

【図面の簡単な説明】

【図１】本発明を適用するシステムの形態図。

【図２】本発明の適用後のシステム形態概要図。

【図３】図２におけるソフトウェア加工処理の具体的フローチャート図。

【図４】図３におけるソフトウェア復元処理の具体的フローチャート図。

【符号の説明】

１００…配布の対象となるソフトウェア、
１０１…サーバに存在しネットワーク上で公開されるソフトウェアの入ったディレクトリ、
１０２…サーバと不特定多数のクライアントが接続されたネットワーク（インターネット）、
１０３…正規の利用者が使うクライアントコンピュータ、
１０４…正規の利用者以外が使うクライアントコンピュータ、
２００…配布の対象となるソフトウェア、
２０１…サーバに存在しネットワーク上で公開されるソフトウェアの入ったディレクトリ、
２０２…サーバと不特定多数のクライアントが接続されたネットワーク（インターネット）、
２０３…正規の利用者が使うクライアントコンピュータ、
２０４…正規の利用者以外が使うクライアントコンピュータ、
２０５…サーバ側でのソフトウェアの加工機能、
２０６…クライアント側でのソフトウェアの自己復元機能、
２０７…加工機能で使用する鍵Ａ、
２０８…正規の利用者のパスフレーズ、
２０９…復元機能で使用する鍵Ｂ、
２１０…ソフトウェア加工後のデータ、
２１１…利用者情報管理データベース、
２１２…鍵Ｂ生成機能、
２１３…鍵管理データベース、
３００…加工処理開始、
３０１…カウンターのクリア、
３０２…鍵Ａの取り込み、
３０３…入力ファイルの１ブロック読込み、
３０４…カウンターのカウントアップ、
３０５…ＥＯＦの判定、
３０６…１ブロックの加工、
３０７…出力ファイルへ追加、
３０８…入力ファイルの１ブロック読込み、
３０９…カウンターのカウントアップ、
３１０…出力ファイルへの自己復元機能の追加、
４００…復元処理の開始、
４０１…カウンターのクリア、
４０２…パスフレーズの取り込み、
４０３…ネットワークの接続、
４０４…鍵Ｂの取り込み、
４０５…鍵Ａの生成、
４０６…入力ファイルの１ブロック読込み、
４０７…カウンターのカウントアップ、
４０８…ＥＯＦの判定、

7

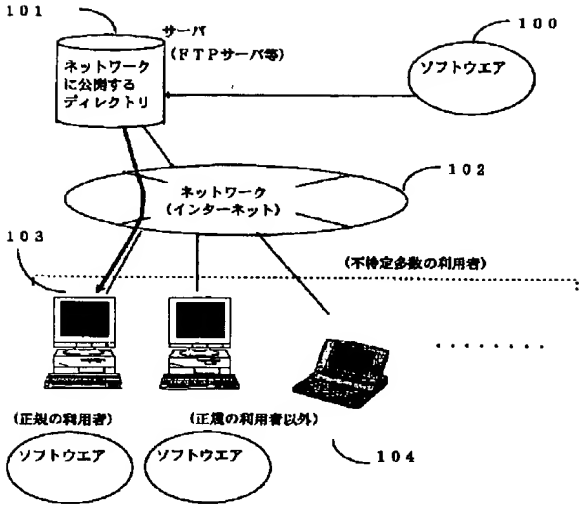
４０９…１ブロックの復元、
４１０…出力ファイルへ追加、

8

＊４１１…入力ファイルの１ブロック読込み、
＊　４１２…カウンターのカウントアップ。

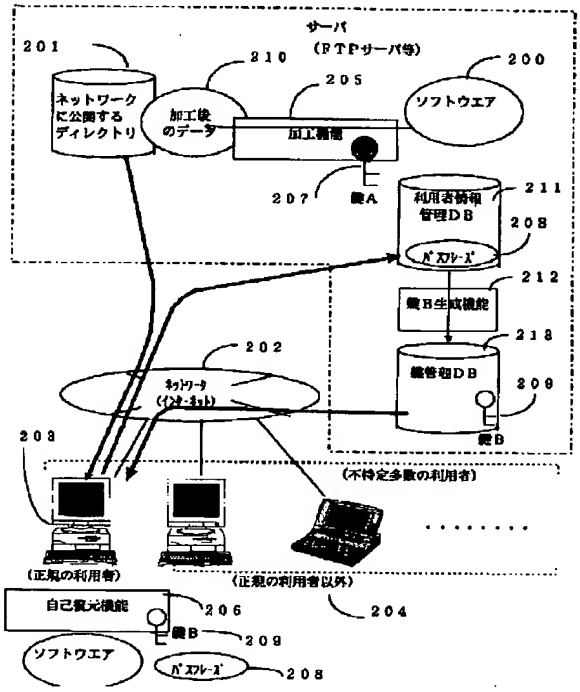
【図１】

図１



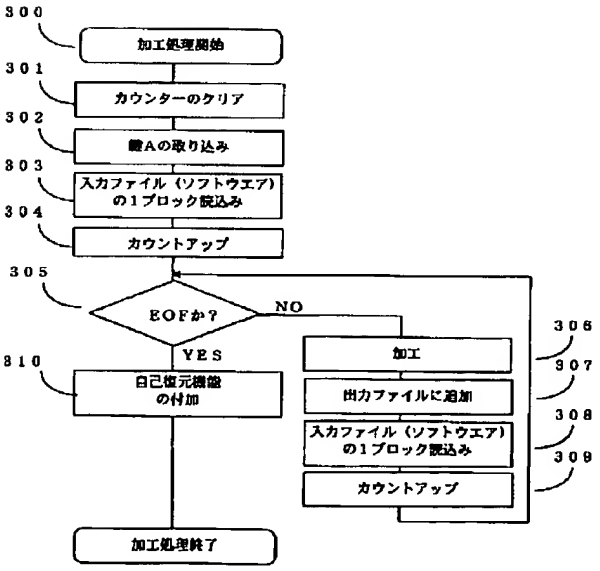
【図２】

図２



【図３】

図３



【図４】

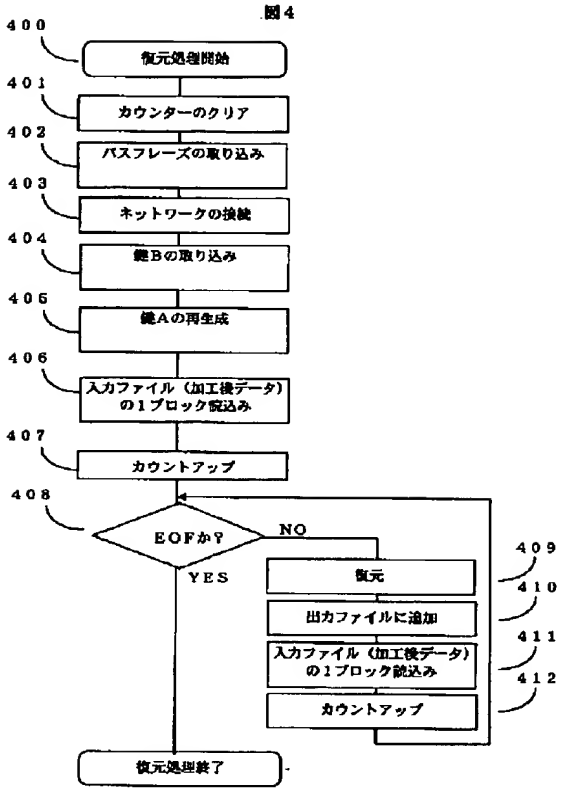


図4
400
復元処理開始
401
カウンターのクリア
402
パスフレーズの取り込み
403
ネットワークの接続
404
鍵Bの取り込み
405
鍵Aの再生成
406
入力ファイル（加工後データ）の１ブロック読込み
407
カウントアップ
408
EOFか？
NO
YES
409
復元
410
出力ファイルに追加
411
入力ファイル（加工後データ）の１ブロック読込み
412
カウントアップ
復元処理終了